Navigating the CRA: A Brief Analysis of European Cyber Resilience Act and Resulting Actions for Product Development

Peter Schoo[a]
Independent Researcher, 82194 Gröbenzell, Germany

Keywords: Cyber Resilience Act, CRA, Product Security, Security Engineering, Harmonised European Standards, Product Certification.

Abstract: This short-paper analyses the forthcoming European Cybersecurity Legislation, focusing on the Cyber Resilience Act (CRA), with an examination of the challenges in defining the CRA addressing product security requirements, life-cycle and supply chain protection, and product criticality classification, that points to certification of product security. Stakeholders, including EU institutions, industry players and Open Source Software (OSS) community, play pivotal roles. The discussion provides a concise but complete overview of the regulatory content and context, the obligations and recommendations for action for companies and practical recommendations for courses at universities, as they arise from the CRA.

1 INTRODUCTION

Enabling technologies are technically harmonised by standards, mostly for ensuring product qualities or to allow for interworking. Regulation determines the legal constrains how products using such technologies are placed on markets according to given standards. Recently the European Union has focused on regulating IT security and data protection for product, platforms and services, which is result of advances in digitisation. For a subset, namely (industrial) cyber-physical products that are placed on European markets the coming CRA will regulate expected and minimum IT security properties. When CRA enters into force and after a transition period, all these products that in the widest sense have digital communication capabilities, will have to come with IT security protection, that will correspond to expected risks, and the maintenance for this protection during the products life time.

The analysis carried out here focuses on the CRA and its profound implications for product development and the realm of IT security. The motivation behind this discussion is to gain a comprehensive understanding of the new legislation, particularly its nuanced consequences for product development and maintenance efforts. As the CRA was recently completed and will now become legally binding, this discussion portrays work in progress and discusses the consequences for vendors that are accessing the European market. While larger enterprises may find these ramifications less pressing and have experiences what is means to follow the security by design paradigm, this discussion may have more significance for Small and Medium-sized Enterprises (SMEs). Additionally, an educational lens will be applied, indicating a thematic direction for security engineering in educational institutions.

The special topic of assessing the implementations of IT security security in a standardised format and from independent 3rd bodies is only touched upon here and not comprehensively discussed. Behind this lies a comprehensive ecosystem, additional procedures, often specific government requirements and further norms and standards that would go beyond the scope of this discussion.

The structure of the discussion is as follows. Commencing with an overview of the legislative landscape and key players involved, the essential ideas encapsulated in the CRA, and subsequently the consequences for the security controls of products are presented. The consideration then extends to scrutinising the impact on the development processes, mandated requirements throughout the product life cycle, and potential product-conformance assessment. The conclusion finally consider indicated actions resulting from the impending CRA, paving the way for a comprehensive understanding of this pivotal cybersecurity legislation.

[a] https://orcid.org/0009-0000-6147-2851

Schoo, P.
Navigating the CRA: A Brief Analysis of European Cyber Resilience Act and Resulting Actions for Product Development.
DOI: 10.5220/0012690500003705

In *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, pages 245-251
ISBN: 978-989-758-699-6; ISSN: 2184-4976

2 UPCOMING EUROPEAN CYBERSECURITY LEGISLATION

In anticipation of secure products for the digital market, the European Commission (EC) has taken decisive steps to bolster cybersecurity, culminating in the EU legislation framework (Figure 1). This legislation encompasses a broad set of regulations, addressing the European market's digital landscape with a focus on products and operational infrastructures. Of this legislation only a subset is discussed here, namely that subset needed here in the discussion for the understanding of the CRA. Initially, the legislation centres with the CSA (European Union, 2019) on a non-sector-specific certification framework for a diverse range of Information and Communications Technology (ICT) devices, processes, and services, excluding regulations on Social Networks platforms. It then extends to cover the protection of Critical Infrastructures (CIs) in European operational sectors and the security of products equipped with networking capabilities, acknowledging with the CRA the increasing relevance of connected industrial IoT devices.

Initially in this legislative initiative, EC published its CRA proposal in 2022 (European Commission, 2022). As result of the consultation process and of the legislative handling in the trilog with the EU institutions , in December 2023 a compromise text (General Secretariat of the Council, 2023) was agreed. The legal text has its entry into force 20 days after being published in the Official Journal of the European Union (OJEU), i.e. the transition period of 36 months and 21 months resp. starts counting. There are two applicability dates the CRA defines. The earlier date is when vendors have to follow security reporting obligation (cmf. Section 3.2). Only after three years the CRA the full applicability will begin for all products placed on the European market by manufacturers, distributors or importers, for selling products to customers or to businesses. For consumers this will be indicated by the CE mark on products to then also including cybersecurity as immanent product properties.

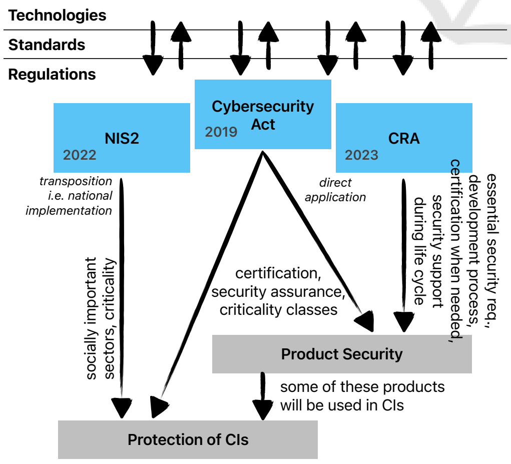

Technologies
Standards
Regulations
NIS2
2022
Cybersecurity Act
2019
CRA
2023
transposition i.e. national implementation
direct application
socially important sectors, criticality
certification, security assurance, criticality classes
essential security req., development process, certification when needed, security support during life cycle
Product Security
some of these products will be used in CIs
Protection of CIs

Figure 1: Simplified EU legislation overview. Acts are directly applicable, Regulations are to be transferred into national legal framework. Cybersecurity Act (CSA) defined in 2019 certification regulation. NIS2 defined in 2022 addresses operation of CI, and draft of December 2023 CRA focuses on security for products that shall be placed in EU market.

> *This regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network* (European Commission, 2022, Article 2).

Such products can also be colloquially referred to as *cyber-physical products*, which is used in he following as synonym.

The CRA relates also to other regulations the EC is committed to and that also address security and data protection. In the three-part criticality grading of AI systems set out in the AI Act [1], the legislature requires that high-risk systems receive IT security protection and resilience as specified by the CRA. This includes AI-specific threats such as data poisoning or adversarial attacks and also risks of fundamental rights. Similar with the Machinery Directive [2] that originally harmonised primarily health and safety requirements for machines, and products that use networking capabilities to support creating data for the European Health Data Space. These machines or devices are considered products with digital elements so that the CRA with its essential requirements to IT security protection is to be applied. Not so Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) that do not have a cyber-physical counterpart. For product developments it then also includes the General Data Protection Regulation (GDPR), to extend the paradigm Security by Design to also Privacy by Design.

Including in this regulatory trajectory is Network and Information Systems Directive (NIS2) (European Union, 2022), concentrating on the safeguarding selected critical infrastructures, which are societal crucial for operational continuity. Member states play a pivotal role in defining national implementation

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri =CELEX:52021PC0206 (in progress)

[2] http://data.europa.eu/eli/reg/2023/1230/oj

plans, tailoring them to the significance and scale of operators within their jurisdictions.

This above arrangement of regulations presents a coherent and streamlined overview of the evolving European cybersecurity landscape over legal frameworks.

3 COMPREHENSIVE REGULATION AFFECTING TECHNICAL IT SECURITY OF PRODUCTS AND THEIR DEVELOPMENT PROCESSES

The CRA represents a new era in European cybersecurity legislation, ending the current practice of simply ignoring the IT security of products. Rather the CRA addresses both technical product properties to build according to *Security by Design* principles and enforce vendors' business processes to maintain security during the life time of products. This is ambitious for a legal framework and builds on scientific grounds and proven security engineering principles and will impact a broad spectrum of products with networking capabilities, including OSS, necessitating a comprehensive set of security disciplines to strengthen the EU market digital landscape. These measures to improve product security are complemented by market monitoring carried out by EC to see how the regulation created by the CRA will work and what acceptance and changes will result.

3.1 Risk-Based Product Cybersecurity Requirements

The cornerstone of the CRA lies in the definition of *product security requirements* depending on the risks a product will be exposed to, e.g. underpinned by a a thorough threat analysis and risk assessment (TARA) that identifies potential threats and results in understanding the products' risks. Dependent on the vendor's risk appetite or the environment the product shall be used in and shall be fit for, the IT security concept for the protection of the product is to be designed and developed.

This can involve documenting crucial security-related decisions, such as the documentation of the TARA and the followed security concept, utilisation of standards, internal security validation, or testing efforts. By requesting such design (intermediate) results, the legislation seeks to establish a robust foundation for the security posture of networked cyber-physical products.

3.2 Maintaining Product Cybersecurity

Security support for products brought to market is a complementing security management aspect in the context of products life-cycle, encompassing the definition of a security support period of five years for vulnerability handling, a well-defined vulnerability disclosure process, and reporting obligations to relevant authorities. Product owners are mandated to adhere to vulnerability handling obligations

- providing products to the market that do not have known actively exploited vulnerabilities, and
- ensuring a swift and effective response to identified vulnerabilities

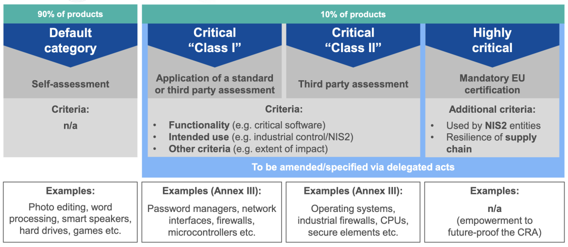
that is expected to release secure products and to help maintaining their protection.

Recognising the interconnected nature of the digital supply chain, the legislation extends its reach to safeguard third-party components, including OSS, against threats such as e.g. potential back-doors, as an responsibility of the product owner. This involves implementing security management practices and introducing a formalised Software Bill of Materials (SBOM). This documentation concept formalises the product construction from components and can also be a chance for the development processes and tools, supporting processing of information about components and enhances transparency within the supply chain.

3.3 Product Cybersecurity Conformance

A significant measure introduced by the CRA is the classification of products based on their criticality (*cmf.* Figure 2). This nuanced approach acknowledges that certain components, like a firewall, carry a higher level of criticality than others, such as e.g. user desktop settings. Compliance with standards and the presentation of fulfilled security requirements, whether claimed or independently assessed by third parties, become paramount in this context. The CRA introduces three classes of products depending on their criticality and an extra class for which EU certification is made mandatory.

It is expected by EC that the majority of products will fall into the class that can self-declare security properties and use of standards. These standards can be *de jure* standards or, a subset of it, specific European standards. However, the identification of such European standards required by the CRA is



90% of products	10% of products		
Default category	**Critical “Class I”**	**Critical “Class II”**	**Highly critical**
Self-assessment	Application of a standard or third party assessment	Third party assessment	Mandatory EU certification
Criteria: n/a	Criteria: • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact)		Additional criteria: • Used by **NIS2** entities • Resilience of **supply chain**
	To be amended/specified via delegated acts		
Examples: Photo editing, word processing, smart speakers, hard drives, games etc.	Examples (Annex III): Password managers, network interfaces, firewalls, microcontrollers etc.	Examples (Annex III): Operating systems, industrial firewalls, CPUs, secure elements etc.	Examples: n/a (empowerment to future-proof the CRA)

Figure 2: Conformity Assessment Classes. Source: European Commission.

in progress to date and their identification is not yet completed by the European Standards Organisations (ESOs). CEN, CENELEC were asked by the EC to identify and name harmonised standard.

With the coming CRA the ESOs will be ask to

> *take into account existing international and European standards for cybersecurity that are in place or under development in order to simplify the development of harmonised standards* (General Secretariat of the Council, 2023, Article 18)

This means that it can be assumed that existing or upcoming standards that can technically meet the essential safety requirements of the CRA will become European standards on which products should then be based accordingly. Advantageously, such harmonised standards then allow the presumption of conformity for products in the Class “Default Category”, i.e. conformity with the essential requirements of CRA can be reasonably assumed. However, it cannot be ruled out that further harmonisation will be necessary in exceptional cases. A risk comparable to the chance that an existing standard will be revised and thereby establish new requirements. In summary, unless a product falls into other classes than “Default Category”, the CE mark requires a self-declaration only [3], which is named to be “internal product control”. Rationals must be part of the vendor’s product documentation that can be presented in case of dispute.

3.4 Critical Product Classes

A self-declaration will not be suitable, however, for critical products, e.g. a firewall. In Annex III the CRA defines the three classes of product types that are *critical products with digital elements* (Critical Class I), *critical products with digital elements* (Critical Class II) and *highly critical products with digital elements*. The (Critical Class II) includes e.g. Micro-controller and -processors, Industrial Automation and Control Systems according to the norm IEC-62443, IIoT (Industrial Internet of Things), robots and smart meter. To assure that such critical products come with claimed security controls that they are suitable according to a given criticality, elements of these classes are more thoroughly assessed. Critical Class I products will require a EC type examination according to the “Module B” and performed by an independent party concerning the conformity to European standards. Critical Class II of critical products will be validated by independent parties according to given security protection profiles that define security requirements and objectives, which are defined independent of the product owner. The highest criticality class is foreseen to assess those products being used in CIs.

To prevent over-regulation and ensure coherence within the legal landscape, the CRA aligns also with other relevant legal acts or directives. Notable connections include the NIS2 for critical infrastructures, the AI Act, and machinery/product safety regulations as mentioned in Section 2.

All of these classifications are based on the assumption that not only the classification is meaningful, but also that (i) compliance with the specific safety requirements is checked uniformly and corresponding to existing certification schemes, and (ii) that there are sufficient capacities to carry out the conformance assessments. For industry both points are most critical in the phase until the CRA enter the full applicability.

3.5 Observe CRA Effect on Market

To monitor and assess the effectiveness of cybersecurity regulations, the CRA introduces a market observation mechanism. With this initiative EC aims to scrutinise the application and impact of the legislation, deciphering its relevance and adaptability of the ever-evolving vulnerabilities of product and ow vendors accordingly act in the European digital landscape. It is a political decision which European agency will receives the responsibility to carry out this market observation.

4 DISCUSSION: CRA CHALLENGES AND OPPORTUNITIES

With completion of the CRA legislation, attention turns to the missing standardisation and opportunities it presents for market stakeholders and the necessary complementary implementation measures.

[3] according to EU Decision 768/2008/EC, “Module A”

4.1 Procedure Defining the CRA

Defining the CRA within the European legislative framework presents a multifaceted set of challenges. As this legal initiative took shape, the European institutions, comprising the EC, the member states Council of the European Union, and the European Parliament, engage as usual in a collaborative process. The EC proposes the legislation, and subsequent discussions involve the Council and Parliament, culminating in a co-decision that shall ensure consensus across all member states and European institutions. Unlike directives, the CRA is a regulation, instantly applicable across member states without the need for national transposition. One of the ambitious task was to complete this initiative in a short period of time and within current parliamentary term of EP and EC, which is, however, not achieved to date as publication in the OJEU has not been done and is only planned.

The distinctive focus on cyber-physical products heightens the complexity of formulating a legal framework, adhering to principles of proportionality and necessity, that addresses essential cybersecurity maintained throughout the life-cycle of products capable of networking, encompassing both hardware and software. On the technical side, the desired essential safety properties for the affected products are already sufficiently covered by R&D, which of course should not exclude any research for further progress. However, the formulation of legal requirements proved to be difficult due to the diverse areas of application of existing products in the consumer sector and for industrial use and due to the different existing business models. A challenge emerged in crafting a framework that genuinely enhances the IT security of diverse products with varying applications and use cases.

Compounding this difficulty was the limited technical security expertise of those formulating and discussing the legal text, overseeing the consequences in applying IT security and for security engineering, and product development to a limited extend only. To bridge this gap, reliance was placed on external security expertise provided by governmental agencies like e.g. ANSSI or German BSI, standardisation bodies, product manufacturing companies, operators of technical systems including the affected OSS community that contributed. For example, *The Apache Software Foundation* participated in the legislative process as a representative of the OSS community and expresses no fundamental dissatisfaction with the outcome of how future IT security requirements for OSS were legally designed (Milinkovich, 2023; van Gulik, 2024). NGOs and civil society were involved to a very limited extent only.

4.2 Standards and Certification

The effectiveness of the CRA legal framework hinges on its alignment with the original goals set by the EC to enhance product security without hindering the European market. Market development will be closely monitored, and the reporting obligations embedded in the CRA and also the NIS2 are expected to significantly improve over the next years observations and statistics of security incidents in both products and deployments. ESO and certification authorities play a pivotal role in the CRA's effectiveness, as the speed of uptake and the establishment of European norms and standards by ESO will be vital. While the set of harmonised European standards is open to date (Har,) regarding the norms the CRA wants to see applied, how shall vendors cope this product development risks in the next years? This will cause enormous uncertainties for industry.

Similar the question for validating and assessing conformity of critical product classes: the development of capabilities and capacities for formal assessments or potential certifications is imperative, as Europe has only very limited organisation (so-called accredited Notified Bodies) that are legitimate to assess the defined conformity. The market at the time being does not have a suitable capacity for assessing the conformity. There are too few companies having been designated to carry out conformity assessment according to a EU directives and it is today questionable if their capacity will be good enough for the massively increasing demand of industry and SMEs. Certification schemes are under way in Europe and it becomes clear that the interest of EC and the affected industries go in different directions. For example, the derived experiences made in applying Common Criteria certification is that this scheme does not fit well to neither evolving ICT systems nor the industrial IoT technology. Evolving ICT systems receive also in future updates that may affect certified security properties. What does this mean for the conformity assessment? Further, IoT systems are build today from many components, from lowest layer processors to eventually user-oriented control components, which establishes a demand for conformity assessments that can follow in a way such component based compositions, avoiding duplication of efforts for security assurance.

4.3 Security Engineering

In order for future products to meet the requirements of CRA, manufacturers and organisations involved in the development of ICT products are obliged to include IT security as early as possible (security by design) and to maintain this protection over the entire product lifespan (security life cycle). It is necessary to define, establish and assess processes of product development, including the supply chains, such that they are compliant to the upcoming regulation. This means first becoming aware of the risks a product must be able to deal with and how the necessary security mechanisms should be designed. Formally, a TARA is required that serves as the basis for the development of a risk-based security concept, which, at the same time, helps avoiding to over-engineer protection efforts.

There are numerous approaches to carry out required threat analysis and risk assessment, e.g. included in EN ISO/IEC 62443, (Common Criteria Organisation, 2017), etc.). There is no agreed method exists for industry or in science, only good practice. Anyhow, it is agreed that the basic scheme follows the scheme:

$$Risk \longleftarrow Threats \times Probability \times Impact$$

The assessment of risks is based on the quality of the threats for (mostly technology induced) attacks, the probability that such threats are expected to come and the expected impact of the attack. To date, such TARA are carried out by experts, however, over time and for given technologies catalogues of threat my be agreed in industry sectors and maintained to follow latest vulnerabilities and identified security flaws, as proposed (Sommer et al., 2019) for the automotive domain to support ISO/SAE 21434.

In order for the security concept to be maintained, it is necessary to be able to update the product or to be able to carry out future updates of used components. This will not necessarily be always successful, especially for legacy products, as examples for an early product end of life indicate. If security support can no longer be provided and updates cannot be made available, then decision may be required for such products to exit the market[4].

The product classes discussed in Section 3.4 help to guide the design of the security concept. Prioritising proven norms and standards not only enhances product security but also simplifies self-declarations, especially for critical product classes, helping to keep certification costs low. This illustrates how important it is harmonised European standards exists and that they are used in products. On the other hand, Class I and below do not require harmonised European standards and can build on standards that are state of the art. This is very important for legacy products that were built but the standards used never fall into the group of harmonised European standards.

All such design and standards application decisions have to be documented well, as it will be needed in case of dispute with market survey agencies. The use of tools for managing product artefacts will help to meet documentation requirements and presents an opportunity to streamline processes for automation, as seen in parts with the SBOM. Specifically when components in the supply chain of a product will be compromised, the product owner is expected to react swiftly and mitigate or eliminate security flaws.

The reporting obligations encompassed in the CRA and that will become early on affecting as mentioned above, will certainly require organisations, vendors and importers adopt their business processes. Practising reporting processes and vulnerability handling within given timelines, aligning such reporting decision processes with also the GDPR obligations indicates some preparation demand and efforts.

4.4 Education and Training

The coming application of the CRA creates demand and impetus for education and training of future IT specialists, specifically in IT security and data protection. The wide-ranging application influences within companies product development, processes, and methods. This includes methods for conducting TARA and using these as basis for defining security concepts that achieve a specified protection level with well-defined remaining risks. Structuring security engineering as part of the development process to encompass predefined security requirements will be crucial, also to adopt to new technologies in the Post Quantum era. It is not the new technology that defines the challenge, but its application and the migration to new technologies.

Being cognisant of duties and obligations arising from vulnerability handling, and understanding liabilities and legal regulations, will play a essential role in shaping the future of digitisation. In essence, the CRA not only mandates compliance but also catalyses a holistic transformation in the approach to cybersecurity, promoting innovation, efficiency, and resilience for products that shall go to European mar-

[4] In another industry, an automaker production of a vehicle type is discontinued because cybersecurity requirements can no longer be fulfilled: https://de.wikipedia.org/wiki/Porsche_Macan or https://www.motor1.com/news/706105/porsche-continuing-gas-macan-sales/ accessed 2024-03-10

ket, and, also this will show effect for all countries the supply chains reaches.

5 CONCLUSION

To conclude, the description compiled here provides a concise but complete overview of the regulatory content and context, the obligations and recommendations for action for companies and practical recommendations for courses at universities, as they arise from the CRA.

In summary, the anticipation remains that this comprehensive legal regulation will not merely touch but fundamentally transform every facet of the IT industry, setting forth a trajectory where security, adaptability, and regulatory adherence converge for a hopefully more resilient digital future. Skills for risk-based Security by Design product development will be key and a major challenge for SMEs. Further, and to date still open, is to quickly define the needed harmonised European standards and certification directives. From the operative perspective vulnerability handling requires to establish an European wide applicable reporting infrastructure that participants can use without too much extra efforts.

When Ursula von der Leyen as president of the EC announced the CRA in September 2021, the draft of which was delivered one year later, she specifically pointed out the need to fight against ransomware. While this threat is not truly addressed by the new legislation, the resistance of connected cyber-physical products against IT security threats will certainly improve for the European market and beyond.

ACKNOWLEDGEMENTS

My thanks go to the patient, anonymous reviewer for the detailed comments that helped making the presentation clearer and easier to understand.

REFERENCES

Harmonised Standards - European Commission. https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en.

Common Criteria Organisation (2017). Common Methodology for Information Technology Security Evaluation – Evaluation methodology, Version 3.1 Revision 5.

European Commission (2022). *Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements For Products With Digital Elements And Amending Regulation (EU) 2019/1020*. European Commission. https://ec.europa.eu/newsroom/dae/redirection/document/89543.

European Union (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act CSA)*. Official Journal of the European Union. EU-Lex Home http://data.europa.eu/eli/reg/2019/881/oj accessed 2024-03-10.

European Union (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council on ENISA and measures for a high common level of cybersecurity across the Union (NIS-2 Directive)*. Official Journal of the European Union. EU-Lex Home http://data.europa.eu/eli/reg/2022/2555/oj accessed 2024-03-10.

General Secretariat of the Council (2023). Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. EU-Lex Home https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_17000_2023_INIT accessed 2024-03-10.

Milinkovich, M. (2023). Good News on the Cyber Resilience Act | Eclipse Foundation Staff Blogs. https://eclipse-foundation.blog/2023/12/19/good-news-on-the-cyber-resilience-act/ accessed 2024-03-10.

Sommer, F., Dürrwang, J., and Kriesten, R. (2019). Survey and Classification of Automotive Security Attacks. *Information*, 10(4):148.

van Gulik, D.-W. (2024). Update on EU Software Regulation: Lots of improvements & good news. https://news.apache.org/foundation/entry/update-on-eu-software-regulation-lots-of-improvements-good-news accessed 2024-03-10.